STATE OF ALABAMA

Information Technology Standard

Standard 650-01S1: Physical Security

1. INTRODUCTION:

Appropriate physical controls must be employed to protect State information system resources from unauthorized access and loss of availability.

2. OBJECTIVE:

Define requirements necessary to implement State IT Policy 650-01: Physical Security.

3. SCOPE:

This Information Technology Standard applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

4. REQUIREMENTS:

4.1 PHYSICAL SAFEGUARDS

Policy: All computer systems, network equipment, and data shall be properly secured to prevent unauthorized physical access and properly safeguarded to protect from loss.

Laptop and portable computers shall be secured with an appropriate physical security device such as a lockdown cable. Computer equipment installed in public areas shall be similarly secured.

Servers, data stores, and other communications equipment shall be placed in secured areas with controlled access.

Access to secured areas shall be controlled by the use of access card keys, access code keypads, or key locks with limited key distribution. A record shall be maintained of personnel who have been granted the access method whether by card, code, or key.

Access codes, where utilized, shall be changed every 90 days or immediately upon removing someone from the approved access list.

Keys, where utilized, shall be closely controlled. If a key is reported as missing, locks shall be changed or re-keyed.

Each facility containing computer and communications equipment shall have a class C fire extinguisher readily available and in working order or an appropriate fire suppression system.

Equipment shall be stored above the floor, in racks whenever feasible, or on a raised floor to prevent damage from dampness or flooding.

Electronic media shall be stored in secured and environmentally controlled areas, in fire safe containers whenever feasible. Backup/archive media shall, whenever feasible, be stored in a secure off-site storage facility.

4.2 PERSONNEL SAFEGUARDS

Policy: Entry into secured areas shall be restricted to authorized-personnel only; other personnel shall be escorted. A log of all visitors granted entry into secured areas shall be maintained and be made available to state security personnel and auditors as needed.

Access to servers and communications equipment shall be limited to authorized technical service personnel. Maintain a list of all personnel authorized to access servers and communications facilities.

Visitors must present Government-issued photo identification, and the information must be recorded to a visitor access log prior to being granted access to secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Visitors must be escorted or in the company of an authorized State employee at all times.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 650-01: Physical Security

6.2 RELATED DOCUMENTS

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	07/14/2006	